

REPUBLICANS

JEFF MILLER, FLORIDA, CHAIRMAN
DOUG LAMBORN, COLORADO
GUS M. BILIRAKIS, ALABAMA
DAVID P. ROE, TENNESSEE
BIL FLORES, TEXAS
JEFF DENHAM, CALIFORNIA
JON RUNYAN, NEW JERSEY
DAN BISHOP, MICHIGAN
TIM HUEBSCAMP, KANSAS
MARK E. AMODEI, NEVADA
MIKE COFFMAN, COLORADO
BRAD R. WENSTRUP, OHIO
PAUL DOKK, CALIFORNIA
JACQUE WALORSKI, INDIANA

JOHN TOWERS, STAFF DIRECTOR

U.S. House of Representatives

COMMITTEE ON VETERANS' AFFAIRS

ONE HUNDRED THIRTEENTH CONGRESS

335 CANNON HOUSE OFFICE BUILDING

WASHINGTON, DC 20515

<http://veterans.house.gov>

January 24, 2014

DEMOCRATS

MICHAEL N. MICHAUD, MAINE, RANKING
CORRINE BROWN, FLORIDA
MARK TAKANE, CALIFORNIA
JULIA BROWNLEY, CALIFORNIA
DINA TITUS, NEVADA
ANN KIRKPATRICK, ARIZONA
PAUL RUIZ, CALIFORNIA
Gloria Nieves McLeod, CALIFORNIA
ANN M. KLISTER, NEW HAMPSHIRE
BETO O'Rourke, TEXAS
TIMOTHY J. WALZ, MINNESOTA

NANCY DOLAN
DEMOCRATIC STAFF DIRECTOR

The Honorable Eric Shinseki
Secretary
U. S. Department of Veterans Affairs
810 Vermont Avenue, NW
Washington, DC 20420

Dear Secretary Shinseki,

I am writing to inform you that, pursuant to an ongoing investigation by the House Committee on Veterans' Affairs, the Committee is requesting information regarding VA's response to the recent eBenefits website privacy and security breach.

It has come to my attention that thousands of Veterans have had their personally identifiable information (PII), including medical and financial information, divulged online through the eBenefits portal. Unfortunately, these types of breaches continue to occur on a regular basis at the VA despite VA's multiple assurances that its systems are secure.

The agency's information systems, including the eBenefits portal, continue to be afflicted by persistent information security weaknesses. Recognizing the importance of securing Veterans' personal information, and minimizing the risk of serious consequences such as identity theft or other fraudulent activity, the Committee expects VA to take all steps necessary to strengthen the security and privacy of the eBenefits portal. As such, please respond to the following questions along with evidentiary documentation by no later than close of business on Friday, January 31, 2014:

1. Please explain in detail how VA identified and addressed the eBenefits 'software defect'.
 - a. In accordance with OMB's Memorandum 07-16, did VA implement their rules of behavior and enforce their table of penalties to anyone for failing to follow the rules for safeguarding PII?
2. In the future, how does VA expect to prevent the same 'software defect' from occurring again?
3. Please explain all previously reported issues with the eBenefits portal, the associated issues, how the issues were fixed (for example, OIT previously used a firewall to address a deficiency in eBenefits) and who was in charge of fixing or repairing the website's weaknesses.
4. How did VA determine that the eBenefits security and privacy breach was the result of a 'software defect' and not a data breach through a system security vulnerability?

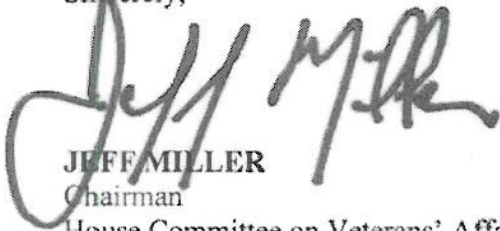
5. Given that 3.4 million Veterans are registered within the eBenefits system, how has VA identified the number of users impacted to be only those using the system at a specific time?
 - a. How many users were logged onto the eBenefits portal during the 'software defect'?
 - b. [REDACTED]
 - c. Per OMB Memorandum 07-16, does VA have the logs of the users who were logged in during the 'software defect'?
6. What specific PII, including medical and financial information, was potentially at risk?
7. Have any Veterans contacted VA providing evidence that their PII was compromised or stolen? If yes, please provide additional detail.
8. Please describe what role the Data Breach Core Team (DBCT) played after the 'software defect' was found.
 - a. In accordance with OMB's memorandum issued on September 20, 2006, did the DBCT engage in a risk analysis to determine whether the incident posed problems related to identity theft?
9. How long was the eBenefits system 'defective'? How long did it take to get the portal back online?
10. After the 'software defect' was identified, did VA do the following, in accordance with OMB Memorandum 06-19 and the Veterans Benefits, Health Care, and Information Technology Act of 2006:
 - a. Report each PII-related breach to Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) within 1 hour of discovery?
 - b. What role is US-CERT currently playing if any to address the 'defect'?
 - c. Please provide evidence that VA notified the Secretary of VA, VA's Chief Information Officer, VA's Office of Inspector General, executives at the Veterans Benefits Administration, Office of Management and Budget, and the House Committee on Veterans' Affairs of the potential PII compromise.
11. Of the 3.4 million Veterans enrolled, how many will be offered credit monitoring services as prescribed within the Veterans Benefits, Health Care, and Information Technology Act of 2006?
12. In accordance with OMB's Memorandum 07-16, did VA determine the level of risk, harm, and impact associated with the potential breach of PII? If so, please describe the risk and the criteria used to assess the level of risk.
13. In accordance with the Veterans Benefits, Health Care, and Information Technology Act of 2006, has the Secretary appointed a non-VA entity or the VA's Inspector General to conduct a risk analysis based on the possible eBenefits privacy and security breach?

14. Has VA consulted and worked with any other agencies (i.e. Department of Defense, Department of Homeland Security, Department of Health and Human Services etc.) to address the problems with the eBenefits portal? If yes, please provide additional detail.
15. As required by the E-Government Act of 2002, has VA conducted an eBenefits privacy impact assessment to show how personally identifiable information is collected, used, shared, and maintained?
16. Does the VA track and keep an inventory of Veterans who have had their PII compromised during past security breaches at VA? If yes, are any of the current casualties of the eBenefits breach also past victims?
17. After the 'software defect' went public and was 'addressed', what did the VA do to regain the trust of the portal's users, as required by OMB's Memorandum 07-16?
 - a. Did the VA provide advice to those potentially affected?
 - b. Did the VA provide any services the agency may provide to those affected?
 - c. Did the VA provide a public notice?
 - d. Did the VA provide a media notice?
 - e. What other steps did VA take to notify the Veterans who may have been affected?
 - f. Since the 'defect' was identified, has the number of users of the portal increased or decreased?
 - g. Does VA have a plan in place to regain the trust of the portal's registered users?
18. Did VA evaluate its response to the eBenefits 'defect' to identify lessons learned and best practices that could be incorporated into its security and privacy policies and practices, as recommended by GAO and described within OMB's Memorandum 07-16? If yes, please provide additional detail on how this was done and a list of the lessons learned. If no, please explain why not.

Please deliver your responses and relevant documentation to our committee office at 335 Cannon House Office Building by the date specified.

If you have any questions or concerns, please contact Jon Towers, Staff Director of the Committee on Veterans' Affairs, at (202) 225-3527.

Sincerely,



JEFF MILLER
Chairman

House Committee on Veterans' Affairs

JM/ah